



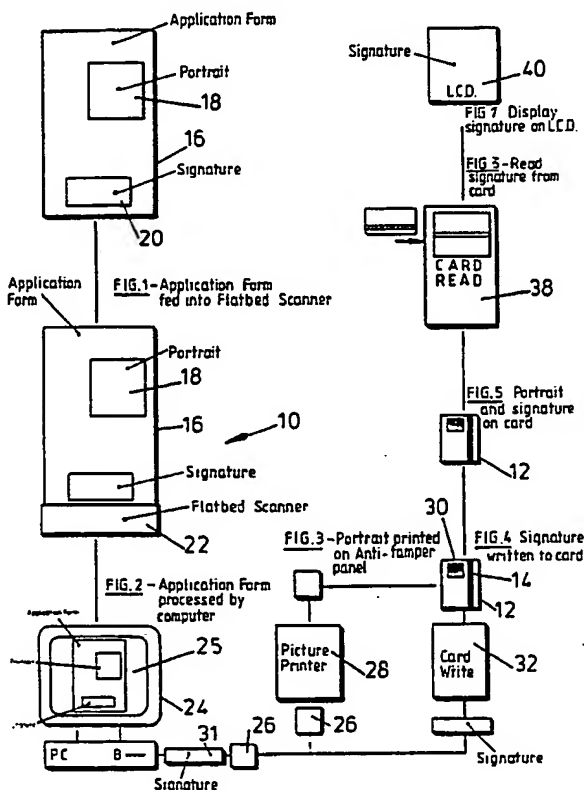
INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

| | | |
|--|---|--|
| (51) International Patent Classification ⁵ : G07C 9/00 | A1 | (11) International Publication Number: WO 92/03804 (43) International Publication Date: 5 March 1992 (05.03.92) |
| <p>(21) International Application Number: PCT/GB91/01385</p> <p>(22) International Filing Date: 14 August 1991 (14.08.91)</p> <p>(30) Priority data: 9017774.2 14 August 1990 (14.08.90) GB 9019544.7 7 September 1990 (07.09.90) GB</p> <p>(71) Applicant (for all designated States except US): SIGNATURE VERIFICATION SYSTEMS LTD. [GB/GB]; Laggan View, Dores Road, Inverness IV1 2DH (GB).</p> <p>(72) Inventor; and (75) Inventor/Applicant (for US only): MACDONALD, John, L. [GB/GB]; 44 Swanston Avenue, Inverness FV3 6QW (GB).</p> <p>(74) Agents: NAISMITH, Robert, Stewart et al.; Cruikshank & Fairweather, 19 Royal Exchange Square, Glasgow G1 3AE (GB).</p> | <p>(81) Designated States: AT, AT (European patent), AU, BB, BE (European patent), BF (OAPI patent), BG, BJ (OAPI patent), BR, CA, CF (OAPI patent), CG (OAPI patent), CH, CH (European patent), CI (OAPI patent), CM (OAPI patent), CS, DE, DE (European patent), DK, DK (European patent), ES, ES (European patent), FI, FR (European patent), GA (OAPI patent), GB, GB (European patent), GN (OAPI patent), GR (European patent), HU, IT (European patent), JP, KP, KR, LK, LU, LU (European patent), MC, MG, ML (OAPI patent), MN, MR (OAPI patent), MW, NL, NL (European patent), NO, PL, RO, SD, SE, SE (European patent), SN (OAPI patent), SU⁺, TD (OAPI patent), TG (OAPI patent), US.</p> <p>Published With international search report.</p> | |

(54) Title: DOCUMENT SECURITY SYSTEM

(57) Abstract

A document security system is described for encoding documents such as credit cards, chargecards and the like with a unique signal representative of the user which cannot be read by the unaided eye and can only be read using a document reading means such as a card swipe machine. In a preferred arrangement the signature (20) of a user is digitised by a digital scanner (22) and the digital data is compressed and magnetically encoded onto the magnetic stripe (14) of the credit card (12). The user's portrait (18) can also be digitised and printed on an anti-tamper panel (30) on the card. In use, the user presents the card (12) in a bank or store and the portrait is initially compared with the user and assuming there is a likeness, the card (12) is swiped through a card-swipe reader (38) and the encoded signature is read and displayed on an LCD-type display (40). The vendor or teller at the point of use can then compare the signature read from the card with the user's actual signature to verify the authenticity of the user. Embodiments of the invention and a novel digital compression technique are described.



+ DESIGNATIONS OF "SU"

Any designation of "SU" has effect in the Russian Federation. It is not yet known whether any such designation has effect in other States of the former Soviet Union.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

| | | | | | |
|----|--------------------------|----|---------------------------------------|-----|--------------------------|
| AT | Austria | ES | Spain | MG | Madagascar |
| AU | Australia | FI | Finland | ML | Mali |
| BB | Barbados | FR | France | MN | Mongolia |
| BE | Belgium | GA | Gabon | MR | Mauritania |
| BF | Burkina Faso | GB | United Kingdom | MW | Malawi |
| BG | Bulgaria | GN | Guinea | NL | Netherlands |
| BJ | Benin | GR | Greece | NO | Norway |
| BR | Brazil | HU | Hungary | PL | Poland |
| CA | Canada | IT | Italy | RO | Romania |
| CF | Central African Republic | JP | Japan | SD | Sudan |
| CG | Congo | KP | Democratic People's Republic of Korea | SE | Sweden |
| CH | Switzerland | KR | Republic of Korea | SN | Senegal |
| CI | Côte d'Ivoire | LJ | Liechtenstein | SU+ | Soviet Union |
| CM | Cameroon | LK | Sri Lanka | TD | Chad |
| CS | Czechoslovakia | LU | Luxembourg | TC | Togo |
| DE | Germany | MC | Monaco | US | United States of America |
| DK | Denmark | | | | |

DOCUMENT SECURITY SYSTEM

The present invention relates to an document security system and apparatus for encoding documents such as cheque cards and credit cards with information to ensure that the documentation can be verified as authentic to prevent document fraud and the like. This invention is particularly, but not exclusively, intended to minimise cheque, cheque card and credit card fraud.

It is well known that document fraud, such as credit card fraud, costs several million pounds per annum both to the owners of the documents such as banks, and also to the customers. In addition, there is considerable police and court time devoted to the pursuit, apprehension and punishment of persons involved in the carrying out of such frauds.

An object of the present invention is to provide a document security system and apparatus which obviates or mitigates the above mentioned problem.

This is achieved by storing a unique signal representative of the user, such as a signature, on the document which cannot be read by the unaided human eye and providing reading means for reading the hidden signal so that the stored signal can be compared with the actual signal.

In a preferred arrangement, the portrait or signature of the user are both provided on the document, for

example, a cheque card or credit card and the signature is encoded on the card so that the signature cannot be read if the document falls into unauthorised hands. However, the encoded signature may be read at the point of use by a reading machine and compared with a stored signature or by direct comparison with the presenter's signature to verify the authenticity of the user.

The user's signature is electronically read and compressed and is stored on a magnetic strip on the document, when the magnetic strip is read at the point of use, the user's signature is displayed on a screen to enable the vendor to compare it with the actual signature of the user to enable verification of the user.

The encoded signal may be optically encoded and consequently can be optically read.

According to one aspect of the present invention there is provided a security system for encoding documents with information representative of a user, said security system comprising,

signal recording means for reading a signal representative of the user onto a document, said signal being digitally encoded so that it cannot be read by the unaided eye, and signal reading means for reading the encoded signal, and display means coupled to the signal reading means for visually displaying the decoded signal so that a comparison between the decoded signal and a further signal provided by the user may be made to verify

the identity of the user.

Conveniently, the signal recording means includes a digital scanner for digitising said signal and a computer coupled to said digital scanner for receiving and storing said digitised signal.

Advantageously, said computer includes digital data compression means for compressing said digital data representative of said signal to a reduced amount of data still representative of said signal, said compressed data being suitable for being magnetically encoded onto the tracks of a magnetic stripe on a document such as a credit card or cheque card.

Preferably, said signal reading means includes magnetic stripe reading means for reading the magnetically coded information on said magnetic stripe.

Preferably also, said magnetic stripe reading means is a card-swipe machine and said displays means is a LCD visual display for displaying the signal read from the document swiped through said card-swipe machine.

The user's signal may be a signature, portrait or fingerprint. Conveniently, the portrait of the user is recorded by said signal recording means and digitised, and printing means are coupled to said computer for receiving said digitised portrait data and printing the portrait of said user on the document as well as the encoded signal to provide a further level of document security.

According to another aspect of the present invention

there is provided a document for use in a document security system said document having a unique signal representative of the user document user, the signal been encoded on the document such that it cannot be read by the unaided eye.

Conveniently, the signal is the user's signature which is magnetically encoded onto a magnetic stripe.

Preferably, the signature data is digitally compressed on said stripe.

According to a further aspect of the invention there is provided a method of storing an encoded signal representative of a user on a machine readable medium comprising the steps of,

digitising the signal representative of the user, and digitally encoding the digitised signal onto the document so that it cannot be ready bhe unaided eye.

Preferably, the method includes the step of compressing the digitised data prior to encoding the digitised signal onto the document.

According to yet a further aspect of the invention there is provided a method of verifying the authenticity of the user of a document comprising,

storing an encoded signal on the document as claimed in any of the claims 19 to 22,

reading the encoded signal from the document with a reading means, and

displaying visually the read signal so that the read

signal can be compared with an actual signal provided by the presenter or user of the document to allow verification of the authenticity of the user.

According to a further aspect of the present invention there is provided a method of compressing a digitised image of a signature comprising the steps of,

setting the desired image size of the signature, setting the level of digital data to fit into said desired signature size;

scanning the digital image of the signature line by line,

on the first scan line removing multiple dots and storing a number of dots and a number of dot displacements;

on the second and subsequent scan lines for each stored dot on the previous line counting and storing increment values, and counting and storing the number and position of stray dots,

comparing the total dot count in the compressed digital data with the digital data level,

scaling the image size of the signature by the target/dot count in the vertical and horizontal scales,

repeating the method steps until the compressed digital data is less than the desired level.

Conveniently, the system includes a plurality of document reading means and display means disposed at remote locations, each document reading means and display means being a stand alone retrieval means for reading the

digitised signal from the document and displaying the retrieval signal.

Conveniently also, each of said plurality of reading and display means are coupled to a central controller whereby the read signal can be electronically compared with a stored signal and both the stored and electronically read signals displayed for a visual comparison.

The image or signature is encoded in optically or magnetically format onto the document and may be read using a magnetic scanner or an optical scanner.

These and other aspects of the invention will become apparent from the following description when taken in combination with the accompanying drawings in which:-

Fig 1 is a schematic diagram of an embodiment of document security system in accordance with present invention;

Figs 2a,2b depict a credit card in accordance with an embodiment of the present invention with the users portrait on the front and the magnetic stripe with the encoded signature on the back.

Fig 3 is a diagrammatic example of a credit card printed with a portrait of a user and which carries a magnetically encoded signature using the system of Fig 1;

Fig 4 depicts a cheque card overprinted with a portrait of a user using the system of Fig 1; and

Fig 5 is a flow chart of a compression algorithm used

with the system of Fig 1 to compress and store signature data on the magnetic strip of a credit card.

Reference is first made to Fig 1 of the drawings which depicts a document security system, generally indicated by reference numeral 10, for incorporating a portrait of the user onto the point of a credit card 12 and the user's signature, invisible to the human eye, onto the magnetic strip 14 on the reverse side of the card, best seen in Figs 2a,2b, as will be later described in detail.

In the system 10, in order to create a secure card 12 a user who wishes such a card completes an application form 16 by including a self-portrait 18 such as a passport-type photograph and also his signature 20. The completed application form 16 is fed into a flatbed image scanner 22 (type M3094 E/P, Fujitsu Limited) which digitises the image data at a fast scanning rate of 200 dots (pixels)/inch resolution in line-art format. The portrait 18 is digitised using grey scale or colour. The digitised data is fed to a personal computer 24 (Apple MacIntosh) which displays the digitised signature on the screen 25. In this format there is far too much data, perhaps 8-20K bytes of data in the signature alone, for it to be recorded onto magnetic card strip.

The digitised portrait information 26 is fed to a picture printer 28 for printing the users portrait on a anti-tamper panel 30 on the front of the credit card 12. The signature 20 is compressed into 160 bytes or

less of information as will be later described and the compressed signature data 31 is fed to a magnetic card write machine 32 which writes the compressed data onto certain available tracks on the magnetic strip 14. In the present case the data is written onto 2 tracks, track 0 and track 4, but this may be varied depending on the particular application. The standard credit card is 3.375" wide and the magnetic strip 14 is the same width. Thus, the data is compressed to fit the magnetic strip width so that for each track there are approximately 200 bits per inch; this is why two tracks are needed to hold 160 bytes of compressed data. It will be appreciated that one byte of the 160 bytes is used as a check sum byte to ensure that data is correctly written to the card or document.

Thus, the security coded credit card 12 contains the users portrait 18 on a tamper-proof panel 30 and the users signature electronically compressed and stored magnetically on tracks 0 and 4 of the magnetic strip 14 as seen in Figs 2a,2b and Fig 3. Similarly, the portrait 18 without the signature may be printed onto personal cheques as shown in Fig 4.

In order to use the card and ensure that the user is authentic, the card is presented to a point of sale position, e.g. the teller in a bank. The teller takes the card and firstly views the card portrait and compares it with the user before him. The card is then passed

through a card reader such as a card swipe machine 38 which has a small LCD T.V. type display 40 coupled thereto. The card read-write machine is not ISO standard having been modified by the addition of switches and firmware inside so that 8 bits can be written to any of the tracks. The users compressed signature is firstly decoded from the tracks and displayed to the teller only on the LCD T.V. type display 40. When the user signs a cheque or other document the teller then compares his actual signature with the card-stored signature and, if satisfied as to the authenticity of the vendor, permits the transaction to be completed. Should the signatures be sufficiently different to cause doubt as to the user's authenticity the vendor may terminate the transaction.

Thus, it will be appreciated that because the signature is invisible to the human eye it cannot be forged and the chances of a fraudulent user being able to sign a duplicate signature to the card-stored signature is negligible. The provision of the users portrait on the credit card further enhances security.

A further level of security may be provided by encoding the digitised portrait or signature to form a scrambled signal and to print the scrambled signal on the cheque, cheque card or other document. At the time of use, the user signs the cheque in the usual way. The scrambled signature cannot be read except by the teller who can "read" the scrambled code with a machine having a

decryption algorithm. The teller is thus able to compare the scrambled signal, representative of portrait or signature, with the stored information. This means that the teller has access to a device either retrieving the unscrambled data from master storage unit or for reading the scrambled information on the document and descrambling it so that a comparison can be made at the point of use.

As described above, a particularly convenient solution to the problem is achieved by printing an unscrambled portrait of the user on the document or card as shown on Figs 2, 3 and 4 for ease of immediate comparison and also providing an unscrambled signal representative of the signature of the user on the card. With existing technology, this comparison can be readily effected in most stores or businesses where document verification is required.

The personal computer 24 and card reader 38 may be connected by a suitable network or other suitable link to a distributed group of computers or terminals which have access to the stored information.

Reference is now made to Fig 5 of the drawings which depicts a flow chart of the compression technique used with the system of Fig 1 to compress the data digitised by the flatbed image scanner 22 to a sufficiently small number of bytes, in our case 160 bytes, to fit onto 2 tracks of the magnetic strip 14 on the credit card 12, but which, when read, will display clearly a legible facsimile

of the actual signature of the user. In practice, the compression technique has to reduce the scanned 200 dots/inch image occupying 8-20K bytes of file space to 160 bytes. The technique parameters could be raised to accommodate higher byte capacities to suit tracks being developed with higher bit densities, for example, 420 BPI instead of 210 BPI. Alternatively, an additional track may be added to the magnetic strip 14 to receive compressed data.

The encoding of magnetic strip is well established and is not disclosed here. Reference is made to an article in Auto ID Today by Sjoerd P. Wouda entitled Magnetic Strip Technology (Vol. 7, June 1989). Because space on each track is limited the compressed data is stored in bit fields which do not fall necessarily on bit boundaries. For example, a 5-bit field could be stored as 3 bits in one byte and 2 bits in the next byte so that no bits are wasted.

Compression of the scanned data is achieved by using the fact that the raster scanned image data is stored as a number of lines of dots. The stored data is first processed, one line at a time, to remove multiple dots which are next to each other as some of these are redundant. For example, a typical pen width at 200 dots/inch scanning results up to 15 to 20 bits in the scanned image and these "multiples" are removed. In addition, the compression technique makes use of the fact that the data in a scanned signature is not random. For

example, in a scanned signature if a dot is encountered in one line, then it is likely that a dot will be found on the next line either directly below or slightly to the right or left. This is resolved down to four possibilities; a dot below, a dot one space left, a dot one space right or none of these and these four possibilities are represented by 2 bits.

Referring to Fig 5, when starting with the first line (line 0) in the image there is a bit field 42 to store a number of points, then a number of bit fields which give the distance to the first point, the distance from the last point to the current point etc. By using the increments algorithm there will be as many increments on the next line (line 1) as points on line 0 so that there is no need for any increment count. Line 1 is therefore scanned 44 for increments and store 46, and then re-scanned 48 to detect any points, called strays, which are not picked-up as increments, and then a further line is encoded in the same format as line 1 with a dot count field plus as many dot displacement fields 50. Thus, line 1 is stored as a dot count plus a bit of dot displacements one line 2 and subsequent lines are stored as a number of increments, each increment being encoded on 2 bits, with the number of increments being the same as the number of dots on the previous line, plus the number of strays and the displacements of those strays.

It is desired to reduce the data to 160 bytes, i.e.

1280 bits and the actual scanned image may contain perhaps 2-300 lines and 6-800 columns. In practice best results have been obtained when this image is scaled down to a maximum of 63 lines by 127 columns. Vertical and horizontal scales are first picked (Fig 4) which match these values and then the image is scanned and compressed. The number of bits in the scanned image is then compared 52 with the target, i.e. 1280 bits in this example. If the number of compressed image bits is greater than the target number of bits, then the number of horizontal and vertical scan lines is scaled down by the number of allowable (target) bits to actual bits 54,56 $(\text{target/dot count HOR; target/dot count VERT})$ so that the target number of bits is obtained in two or three iterations. If the number of compressed image bits is less than the target number, the compression is complete.

The technique contains several optimisation features, one of which is that the bit fields are reduced in size from the theoretical minimum to save space. For example, because more than 15 strays are rarely encountered on one line, the count of strays is encoded on 4 bits only. If there is a stray count >15 in the 4-bit field, 15 is put in the 4-bit field and then the next 6-bit field is used for the full stray count. Therefore, on that particular line storage capacity has been lost, but overall the technique has saved 5 to 10% of storage. The same technique is also applied to the storage of displacements

on a line.

It will be understood that various modifications may be made to the embodiment herebefore described before departing from the scope of the invention. In the apparatus described, for example, a video camera could be used for taking portraits and the image scaled to provide a digitised portrait. Alternatively, a still photograph or signature could be digitised using a digitising tablet. In addition, the flatbed image scanner 22 may be used to digitise a picture of the fingerprint of a user to provide a unique signal representative of that user and this signal compressed using a similar technique described with reference to the signature. A similar compression technique may be used to compress the portrait data. The compressed data may be optically encoded onto the document and read by an optical card reader (OCR) using existing OCR technology. The photograph and/or image of the user may be located on the signature strip on a credit card and the scrambled code may be contained in a medium which can be decoded by an optical scanner or magnetic scanner.

The laser printer may be replaced by any other suitable digitally controlled printer such as an ink-jet printer or electro-static printer. In addition, it is not necessary for other remote terminals to be directly connected to a master computer which stores all the information or a stand-alone reader to compare the

presenters signature with that which is encoded. The remote terminals may be connected by a modem. The information may be stored on a disc which may be sent to a remote location and inserted into an appropriate host terminal which has software to enable the comparisons of portrait and encoded signature to be made with the presenters signature. Signatures or portraits could also be faxed to remote locations from a central location to facilitate verification. It will be understood that document is a general term applicable to a variety of objects such as credit cards, smart cards, chargecards, cheques, cheque guarantee cards, files, folders, I.D. cards, security access cards and any other suitable document where it is desirable to ensure the authenticity of the user and prevent fraud.

Advantages of the present invention are that there are extra levels of security to enable verification of the user to take place and that the comparison is effected on the basis of characteristics which are believed to be unique to the user, for example, the portrait signature, fingerprint or combinations of these. Thus, the opportunity for forgery or fraud in connection with such documentation is considerably minimised. The system uses existing technology and is designed to interface with existing systems, thus it can readily be set up in existing environments without specialist expertise.

In the case of a smart card, i.e. one that has a

processor and storage means, the signature and portrait
could be contained in the storage means therein.

CLAIMS

1. A security system for encoding documents with information representative of a user, said security system comprising,

signal recording means for reading a signal representative of the user onto a document, said signal being digitally encoded so that it cannot be read by the unaided eye, and signal reading means for reading the encoded signal, and displays means coupled to the signal reading means for visually displaying the decoded signal so that a comparison between the decoded signal and a further signal provided by the user may be made to verify the identity of the user.

2. A security system as claimed in claim 1 wherein the signal recording means includes a digital scanner for digitising said signal and a computer coupled to said digital scanner for receiving and storing said digitised signal.

3. A security system as claimed in claim 1 or claim 2 wherein said computer includes digital data compression means for compressing said digital data representative of said signal to a reduced amount of data still representative of said signal, said compressed data being suitable for being magnetically encoded onto the tracks of

a magnetic stripe on a document such as a credit card or cheque card.

4. A security system as claimed in preceding claim wherein said signal reading means includes magnetic stripe reading means for reading the magnetically coded information on said magnetic stripe.

5. A security system as claimed in claim 5 wherein said magnetic stripe reading means is a card-swipe machine and said displays means is a LCD visual display for displaying the signal read from the document swiped through said card-swipe machine.

6. A security system as claimed in any preceding claim wherein the users signal is a signature.

7. A security system as claimed in any preceding claim wherein the users signal is a portrait or a fingerprint.

8. A security system as claimed in any preceding claim wherein the portrait of the user is recorded by said signal recording means and digitised, and printing means are coupled to said computer for receiving said digitised portrait data and printing the portrait of said user on the document as well as the encoded signal to provide a further level of document security.

9. A security system as claimed in any preceding claim wherein the signal recording means includes data encryption means for encrypting said digital data prior to encoding said digital data onto said document, and said data reading means including data decrypting means for decrypting the encrypting data on said document.

10. A security system as claimed in claim 8 or claim 9 wherein said printing means is a laser printer.

11. A security system as claimed in any preceding claim wherein said document is a credit card, cheque card or smart card and which has a magnetic stripe with the signature of the user encoded thereon and a portrait of the user printed thereon.

12. A document for use in a document security system said document having a unique signal representative of the user document user, the signal been encoded on the document such that it cannot be read by the unaided eye.

13. A document claimed in claim 12 wherein the signal is the user's signature which is magnetically encoded onto a magnetic stripe.

14. A document as claimed in claim 13 wherein the

signature data is digitally compressed on said stripe.

15. A document as claimed in any one of claims 12 to 14 wherein the document has a portrait of the user thereon.

16. A document as claimed in claim 15 wherein the portrait is contained in a tamper-proof panel.

17. A document as claimed in any one of claims 13 to 16 wherein the user's signature is encoded onto 2 tracks of said magnetic stripe.

18. A document as claimed in any preceding claim wherein said document is a credit card, cheque card or smart card with a magnetic stripe thereon.

19. A method of storing an encoded signal representative of a user on a machine readable medium comprising the steps of,

digitising the signal representative of the user,
and digitally encoding the digitised signal onto the document so that it cannot be read by the unaided eye.

20. A method as claimed in claim 19 wherein the method includes the step of compressing the digitised data prior to encoding the digitised signal onto the document.

21. A method as claimed in any preceding claim where the digitised signal is magnetically encoded onto the document.

22. A method of verifying the authenticity of the user of a document comprising,

storing an encoded signal on the document as claimed in any of the claims 19 to 22,

reading the encoded signal from the document with a reading means, and

displaying visually the read signal so that the read signal can be compared with an actual signal provided by the presenter or user of the document to allow verification of the authenticity of the user.

23. A method as claimed in any one of claims 19 to 22 wherein the user's signature is a unique signal representative of the user.

24. A method of compressing a digitised image of a signature comprising the steps of,

setting the desired image size of the signature,
setting the level of digital data to fit into said desired signature size;

scanning the digital image of the signature line by line,

on the first scan line removing multiple dots and
storing a number of dots and a number of dot displacements;

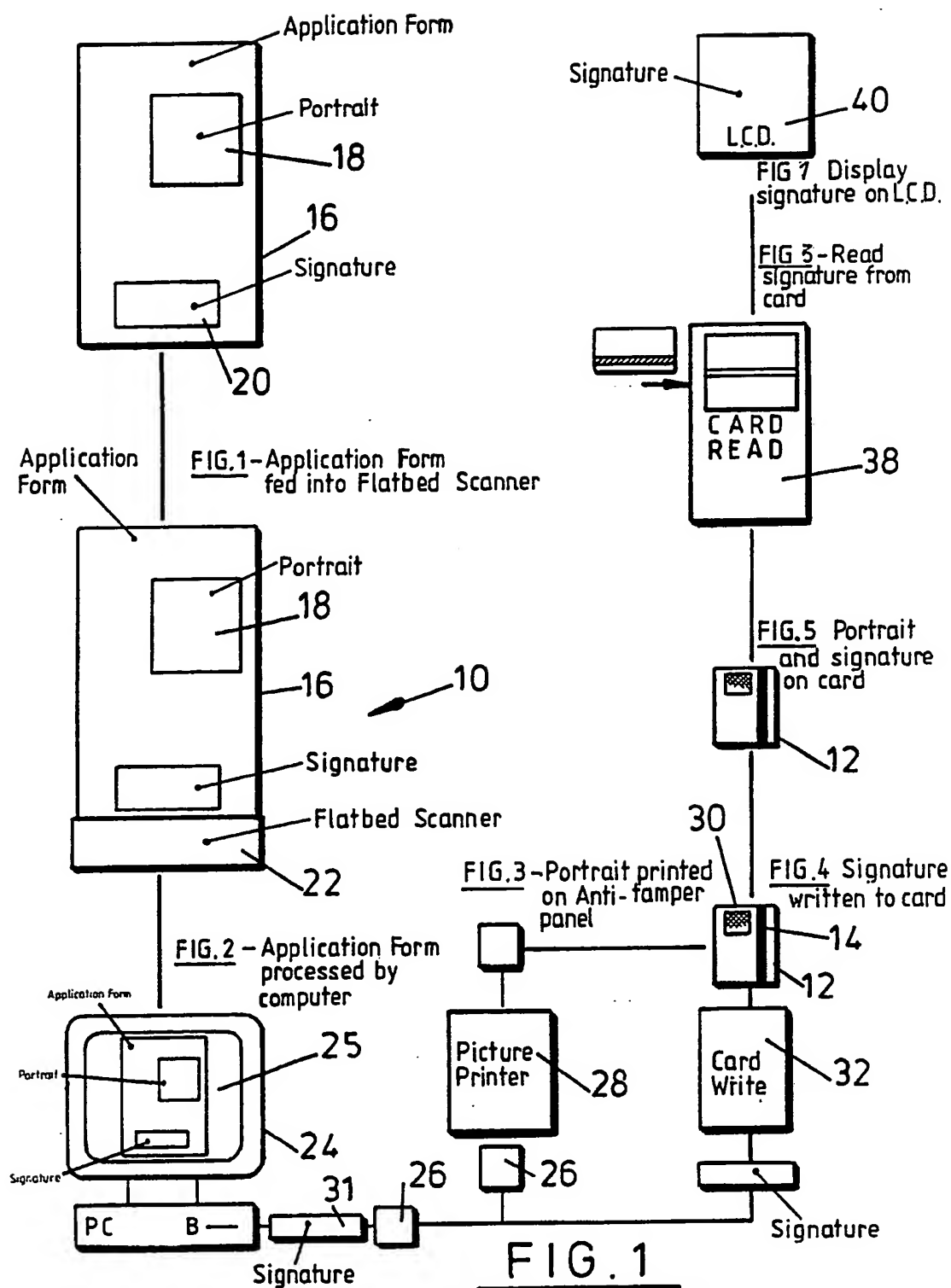
on the second and subsequent scan lines for each dot on the previous line counting and storing increment values, and counting and storing the number and position of stray dots,

comparing the total dot count in the compressed digital data with the digital data level,

scaling the image size of the signature by the target/dot count in the vertical and horizontal scales,

repeating the method steps until the compressed digital data is less than the desired level.

1 / 4



2 / 4

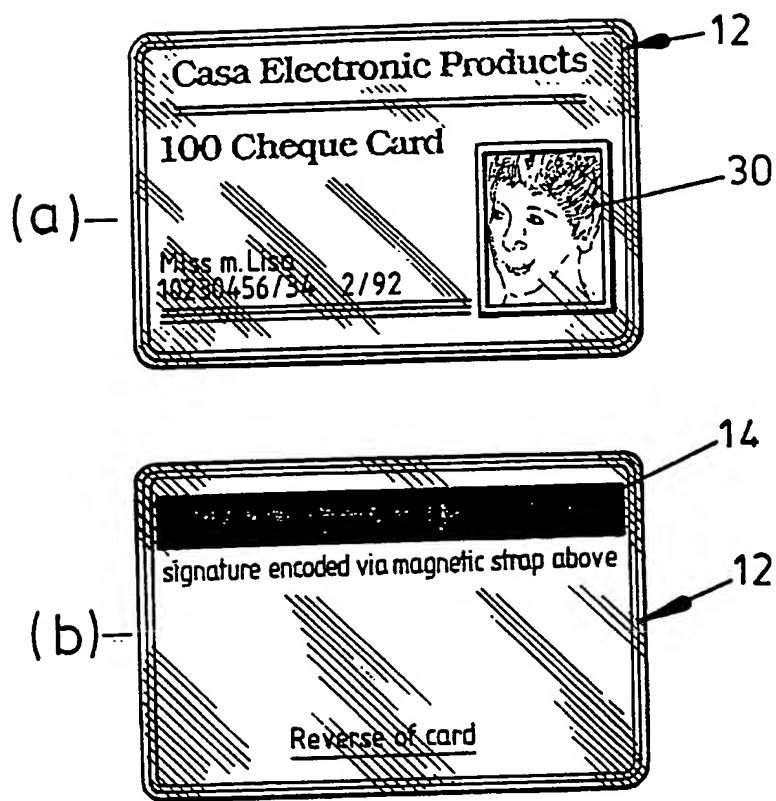
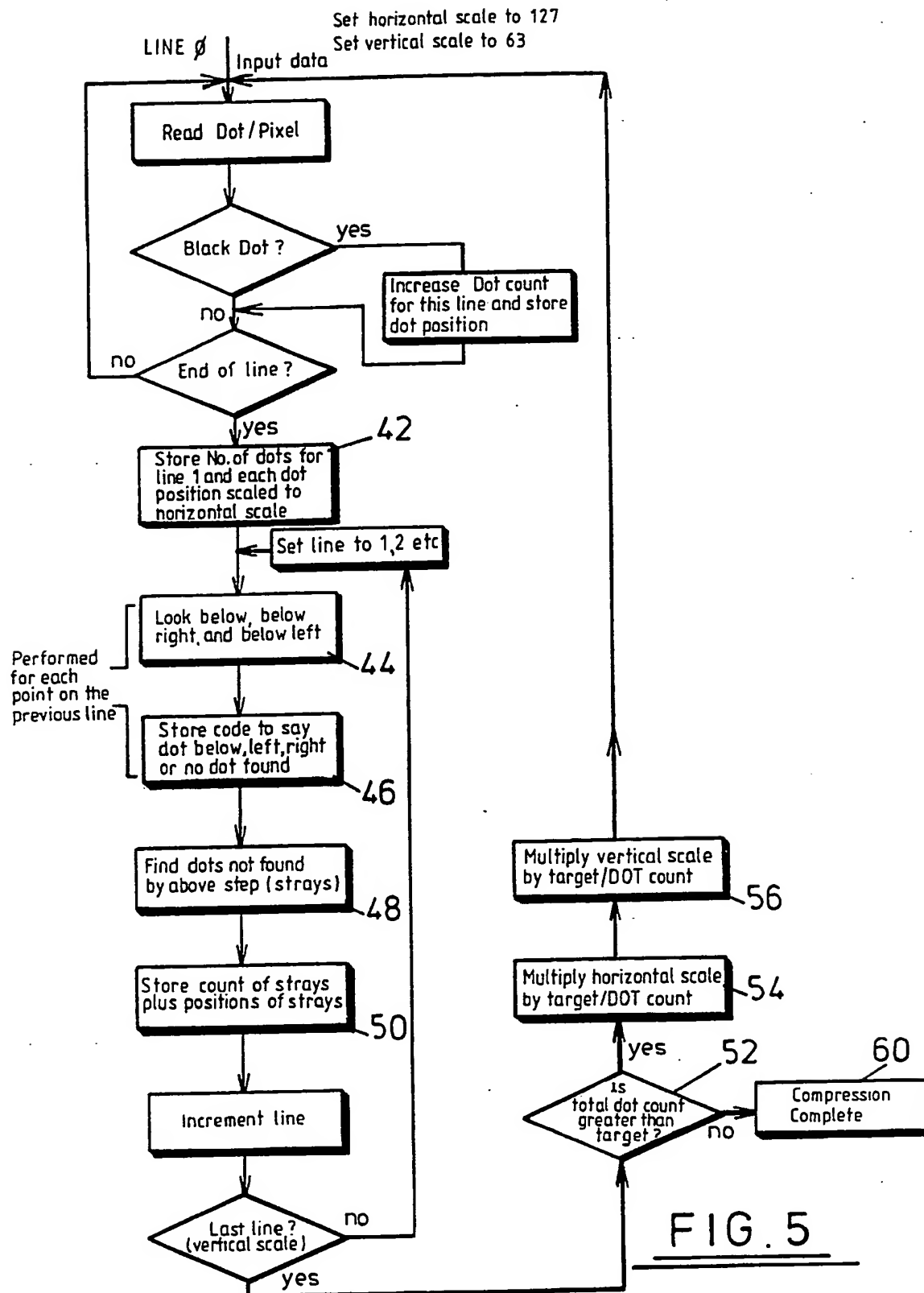


FIG. 2

4 / 4




SUBSTITUTE SHEET

INTERNATIONAL SEARCH REPORT

International Application No

PCT/GB 91/01385

| | | |
|---|--|---|
| I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) ⁶ | | |
| According to International Patent Classification (IPC) or to both National Classification and IPC | | |
| Int.Cl. 5 G07C9/00 | | |
| II. FIELDS SEARCHED | | |
| Minimum Documentation Searched ⁷ | | |
| Classification System | Classification Symbols | |
| Int.Cl. 5 | G07C ; B42D ; G06K | |
| Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched ⁸ | | |
| III. DOCUMENTS CONSIDERED TO BE RELEVANT⁹ | | |
| Category ¹⁰ | Citation of Document, ¹¹ with indication, where appropriate, of the relevant passages ¹² | Relevant to Claim No. ¹³ |
| X | WO,A,8 900 741 (ETC) 26 January 1989 see page 1, line 24 - page 3, line 11 see page 4, line 5 - page 12, line 14 see page 14, line 23 - page 15, line 33; figures | 1-7 12-14 17-23 |
| Y | | 8,10,11 15,16 9,24 |
| A | --- | |
| X | EP,A,0 334 616 (LEIGHTON) 27 September 1989 see column 2, line 8 - column 8, line 44 see figures | 1-4 7-9 11,12 15-22 5 24 |
| Y | | |
| A | --- | |
| | --- | |
| | -/- | |
| ¹⁰ Special categories of cited documents : "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date. "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art. "&" document member of the same patent family | | |
| IV. CERTIFICATION | | |
| Date of the Actual Completion of the International Search | Date of Mailing of this International Search Report | |
| 03 DECEMBER 1991 | 11. 12. 91 | |
| International Searching Authority | Signature of Authorized Officer | |
| EUROPEAN PATENT OFFICE | MEYL D.  | |

| III. DOCUMENTS CONSIDERED TO BE RELEVANT (CONTINUED FROM THE SECOND SHEET) | | |
|--|---|--|
| Category * | Citation of Document, with indication, where appropriate, of the relevant passages | Relevant to Claim No. |
| X | IBM TECHNICAL DISCLOSURE BULLETIN. vol. 30, no. 8, January 1988, NEW YORK US page 366; 'FACIAL IMAGE DATA ON CREDIT CARD FOR IDENTIFICATION' see the whole document | 1-4,7, 10, 12-15, 17-21 |
| A | --- | 24 |
| X | FR,A,2 592 197 (NIXON) 26 June 1987 see page 6, line 5 - page 7, line 31 see page 9, line 27 - page 13, line 10; figures | 1,2,6,8 9,12,15 18-20, 22,23 3,4,14, 24 |
| A | --- | |
| Y | IBM TECHNICAL DISCLOSURE BULLETIN. vol. 31, no. 7, 7 December 1988, NEW YORK US pages 441 - 442; 'PERSONAL IDENTIFICATION TERMINAL' see the whole document | 5 |
| Y | FR,A,2 449 930 (GAO) 19 September 1980 see page 12, line 11 - page 13, line 4; figures | 8,10,11 15,16 |
| A | WO,A,8 703 724 (GAMMA SYSTEMS) 18 June 1987 | |
| A | WO,A,8 204 149 (HARRISON) 25 November 1982 | |
| | --- | |

**ANNEX TO THE INTERNATIONAL SEARCH REPORT
ON INTERNATIONAL PATENT APPLICATION NO. GB 9101385
SA 50489**

This annex lists the patent family members relating to the patent documents cited in the above-mentioned international search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information. 03/12/91

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date | |
|---|---------------------|----------------------------|---------------------|----------|
| WO-A-8900741 | 26-01-89 | AU-A- | 2126088 | 13-02-89 |
| | | EP-A- | 0330684 | 06-09-89 |
| | | JP-T- | 2501098 | 12-04-90 |
| ----- | | | | |
| EP-A-0334616 | 27-09-89 | US-A- | 4879747 | 07-11-89 |
| | | JP-A- | 2028775 | 30-01-90 |
| | | US-A- | 4995081 | 19-02-91 |
| ----- | | | | |
| FR-A-2592197 | 26-06-87 | None | | |
| ----- | | | | |
| FR-A-2449930 | 19-09-80 | DE-B- | 2907004 | 21-08-80 |
| | | AT-B- | 384781 | 11-01-88 |
| | | AT-B- | 388707 | 25-08-89 |
| | | BE-A- | 881878 | 16-06-80 |
| | | CH-A- | 646536 | 30-11-84 |
| | | GB-A, B | 2044175 | 15-10-80 |
| | | JP-A- | 55146795 | 15-11-80 |
| | | NL-A- | 8001018 | 26-08-80 |
| | | SE-B- | 451220 | 14-09-87 |
| | | SE-A- | 8001410 | 23-08-80 |
| | | US-A- | 4544181 | 01-10-85 |
| ----- | | | | |
| WO-A-8703724 | 18-06-87 | AU-A- | 6524486 | 30-06-87 |
| | | EP-A- | 0248032 | 09-12-87 |
| ----- | | | | |
| WO-A-8204149 | 25-11-82 | EP-A- | 0079354 | 25-05-83 |
| | | GB-A- | 2101931 | 26-01-83 |
| ----- | | | | |